3 ביוני 2012
י"ג סיון תשע"ב

טיוטה של תקנות אבטחת מידע לפי חוק הגנת הפרטיות
בעקבות הערות הציבור לנייר עמדה בעניין זה

רמו"ט ומחלקת ייעוץ וחקיקה במשרד המשפטים מפרסמות היום טיוטה של תקנות אבטחת מידע לפי חוק הגנת הפרטיות לעיון הציבור. טיוטת התקנות הוכנה לאחר קבלת הערות מהציבור לנייר עמדה שהפיצה רמו"ט בעניין זה, ומפנימה גם לקחים מפרשת "ההאקר הסעודי".

חוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק), קובע הוראות שונות וחובות בתחום אבטחת המידע על מי שמנהל מידע אישי באופן ממוחשב, שמטרתן צמצום החשש מפני שימוש לרעה או פגיעה במידע.

מטרת התקנות המוצעות היא לפרט ולקבוע את עקרונות אבטחת המידע הקשורים בניהול ובשימוש במידע אישי, בהתבסס על תקני אבטחת מידע מקובלים בעולם.
המטרה של ההסדר המוצע הוא **מימוש תכלית ההגנה על הפרטיות במידע** - כלומר הגנה על זכויות אנשים שפרטים עליהם מצויים במידע במאגר המידע, מפני שימוש לרעה במידע אודותיהם הן על ידי גורמים מחוץ לארגון, והן על ידי עובדים בו.

רמו"ט הפיצה נייר עמדה בעניין זה להערות הציבור בפברואר 2010 והציגה אותו בימי עיון שארגנה ובכנסים מקצועיים אחרים. לנייר העמדה התקבלו הערות מגורמים שונים במגזר הציבורי והעסקי. הליך שמיעת הערות הציבור הביא לשינויים בדרישות המוצעות.

התקנות המוצעות כוללות הסדרה במישור התהליכים וקבלת ההחלטות בתוך הארגון, וכן הוראות מהותיות בתחום ניהול אבטחת המידע:

במישור האחריות הארגונית, ובהתאם להוראות סעיף 17 לחוק, נקבע כי האחריות הכוללת לעמידה בתקנות היא של בעל מאגר המידע (כלומר הגוף הציבורי או הפרטי שאוסף ומעבד את המידע) ומנהל המאגר (כלומר מנכ"ל הגוף או בכיר אחר שהוא הסמיך לכך). כמו כן, החובות יחולו באופן דומה גם על המחזיק במאגר מידע. חידוש שנובע מהערות שהתקבלו מקהילת

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

אבטחת המידע, קשור ביחסי הגומלין שבין מנהל המאגר לממונה אבטחת המידע. נדרש כי ממונה אבטחת המידע יהיה כפוף לנושא משרה בכיר. עוד נדרש בעל מאגר המידע להקצות לממונה אבטחת המידע את המשאבים הנדרשים לביצוע תפקידיו.

כלקח מאירועי אבטחת המידע הקשורים בפרשה שידועה כ-"האקר הסעודי" נדרשים ארגונים להכין נהלי התמודדות עם אירועי אבטחת מידע. בנוסף, באירועי אבטחת מידע חמורים בלבד, מוצעת חובת דיווח על כך לרשם מאגרי המידע, ובכלל זה הצעדים המתקנים שננקטו (Breach Notification Notice). הרשם יוכל גם להורות על מסירת הודעה על כך לציבור שעלול להיפגע מן האירוע.

נושאים נוספים ששונו וחלו בהן הקלות למול נייר העמדה עוסקים בתדירות ניהול סקרי סיכונים, חובות בתחום המידור וחובות ניטור ומעקב כוללות על השימוש במערכות.

בשל מגוון הארגונים המעבדים מידע אישי, התקנות המוצעות הן מודולריות, בכך שהן מחילות חובות ברמה הולכת וגדלה ככל שהארגון הוא ארגון שפעילות עיבוד המידע שבו, בהקשר של חוק הגנת הפרטיות, היא משמעותיות יותר. תפיסה זו, של חובות מודולריות נגזרת ישירות מעקרון היסוד של אבטחת מידע שלפיה התמודדות עם סיכוני האבטחה נבחנת בהתאם לפעילות של המאגר, והיא מוצאת ביטויה גם במסמכים דומים בעולם. סיווג הגדרות המאגרים בהתאם למידת רגישות המידע שבמאגר הותאם לנוסח הצעת חוק הגנת הפרטיות (תיקון מספר 12) (סמכויות אכיפה), התשע"ב-2011, וכן לשינויים בחובות המוצעות לפי התקנות.

התקנות מופצות להערות הציבור תוך 21 יום, ולאחר מכן יובאו לאישור שר המשפטים.

הערות יש להעביר עד ליום 24/06/2012 באמצעות דוא"ל לכתובות הבאות: **ilita@justice.gov.il** ו- **YeutzHakika@justice.gov.il** ולציין בכותרת הדוא"ל "תקנות אבטחת מידע - הערות".

ההערות תועברנה גם למחלקת ייעוץ וחקיקה במשרד המשפטים ותפורסמנה באתר רמו"ט

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

מעודכן 5.4.2012

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ב- 2012

בתוקף סמכותי לפי סעיף 36 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן - החוק), ובאישור ועדת חוקה חוק ומשפט של הכנסת, אני מתקין תקנות אלה:

הגדרות	1.	בתקנות אלה -
		"חומר מחשב", "מחשב" ו"פלט" – כהגדרתם בחוק המחשבים, התשנ"ה- 1995[1].
		"עובד" - יחיד המועסק על ידי בעל מאגר או מחזיק, לרבות מי שעימו התקשר בעל מאגר לפי תקנה 15, במישרין או בעקיפין, ואשר יש לו גישה לאחד מאלה ביחס למאגר מידע על פי הרשאתו של בעל המאגר או המחזיק: (1) מידע; (2) מערכות המחשוב של המאגר (3) מידע או רכיב הנדרש לצורך הפעלת המאגר או לצורך גישה אליו;
		"נושא המידע" – האדם אודותיו קיים מידע במאגר המידע.
		"התקן נייד" - אחד מאלה:

(1) מחשב המיועד לשימוש נייד ובכלל זה רדיו טלפון נייד כהגדרתו בחוק התקשורת (בזק ושידורים) התשמ"ב-1982 ;

(2) מצע אחר המשמש לאחסון חומר מחשב;

		"מאגרים שחלה עליהם רמת האבטחה הבינונית" - מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה;
		"מאגרים שחלה עליהם רמת האבטחה הגבוהה" - מאגרי מידע מן הסוגים המפורטים בתוספת השנייה;
		"תקן ישראלי" - כמשמעותו בחוק התקנים, התשי"ג-1953[2].
	2.	(א) בעל מאגר יגדיר במסמך הגדרות מאגר (להלן – מסמך הגדרות המאגר), לכל הפחות, את כל העניינים האלה:
		(1) תיאור כללי של פעילות איסוף ושימוש במידע לצורך פעילות בעל המאגר (להלן – פעולות שימוש במידע);
		(2) תיאור מטרות השימוש במידע;

[1] ס"ח התשנ"ה, עמ' 366.
[2] ס"ח התשי"ג, עמ' 30.

			(3) תיאור של סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 1(3) לתוספת הראשונה, ומידת הנזק הצפויה לפרטיות נושא המידע בשל פגיעה באבטחת המידע במאגר ביחס למידע זה;
			(4) פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה- מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר;
			(5) פירוט לעניין ביצוע פעולות עיבוד מידע באמצעות מחזיק;
			(6) הסיכונים המרכזיים לפגיעה באבטחת המידע ואופן ההתמודדות עם סיכונים אלה;
			(7) שמו של מנהל המאגר ושל הממונה על אבטחת מידע במאגר אם מונה כזה.
			(ב) בעל מאגר יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי בנושאים המפורטים לעיל, ויבחן את הצורך בעדכון כאמור בכל שנה קלנדרית, בשל שינויים טכנולוגים ארגונים או אירועי אבטחה כאמור בתקנה 11, עד ל – 31.12 לאותה שנה.
			(ג) בעל מאגר יבחן אחת לשנה כי המידע הנשמר על ידו במאגר אינו מעבר לנדרש לצורך מטרות המאגר.
3. ממונה על אבטחת מידע			במידה שחלה חובה למנות ממונה על אבטחת מידע, או שמונה ממונה על אבטחת מידע במאגר המידע (להלן – ממונה על אבטחה) יחולו הוראות אלה:
			(א) הטיל בעל מאגר על ממונה על אבטחה משימות לשם ביצוע תקנות אלה, הנוספות על החובות המנויות בסעיפים קטנים (ד) ו-(ה), יגדירן בצורה ברורה ויקצה לרשות הממונה את המשאבים הדרושים לו לשם מילוי תפקידו; (ב) לא יתמנה ממונה על אבטחה אלא אם הוא כפוף ישירות למנהל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר, באופן שיבטיח את עצמאותו המקצועית; (ג) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה; (ד) הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר; (ה) הממונה יכין תכנית לבקרה שוטפת על העמידה בהוראות תקנות אלה, יבצעה ויודיע לבעל המאגר ולמנהל על ממצאיו.

נוהל אבטחה	4.	(א) בעל המאגר יקבע נוהל אבטחת מידע (להלן – נוהל האבטחה) בהתאם למסמך הגדרות המאגר ולתקנות אלה.
		(ב) בעל המאגר יורה כי נוהל האבטחה יחייב את כל העובדים; נוהל האבטחה יישמר כך שפרטים ממנו יימסרו לעובדים רק בהיקף הנדרש לצורך ביצוע תפקידם.
		(ג) נוהל האבטחה יכלול, בין היתר, התייחסות לכל אלה:
		(1) פרטים כאמור בתקנה 5 (א);
		(2) קביעת הרשאות גישה למידע במאגר, למערכות תשתית המחשוב, תקשורת ואבטחת המידע בהתאם לתקנה 8;
		(3) תיאור של אמצעים שמטרתם הגנה על מערכות המחשוב ותשתיות התקשורת של המאגר ואופן הפעלתם לצורך כך;
		(4) הוראות למורשי הגישה למאגר המידע, תשתיות המחשוב, התקשורת ואבטחת המידע לצורך הגנה על המידע במאגר;
		(5) הסיכונים להם חשוף המידע במסגרת הפעילות השוטפת של בעל המאגר, לרבות אלה הנובעים ממבנה מערכות המאגר, אופן קביעת סיכונים אלה, ואופן הטיפול בסיכונים אלה, לרבות בדרך של יישום מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות רגישות הקשורות אליו;
		(6) אופן התמודדות עם אירועי אבטחת מידע, בהתאם לחומרת האירוע ולמידת רגישות המידע, כאמור בתקנה 11;
		(7) הוראות בעניין האבטחה הפיסית והסביבתית של מתקני המאגר כאמור בתקנה 6.
		(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול נוהל האבטחה, בנוסף לאמור בתקנת משנה (ג), התייחסות גם לכל אלה:
		(1) אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המחשוב של המאגר;
		(2) הוראות לעניין ניהול והעברה של אמצעי אחסון והתקנים ניידים;

			(3) הוראות לעניין היבטי אבטחת מידע הקשורים בגיבוי המידע;
			(4) הוראות לעניין ביצוע ביקורות תקופתיות כדי לוודא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה.
			(5) הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה הגישה של אנשי הפיתוח לנתונים במאגר.
			(ה) בעל מאגר יבחן את הצורך בעדכון הנוהל אחת לשנה; מבלי לגרוע מהאמור, בעל המאגר יבחן אם יש צורך בעדכונו של הנוהל במקרים אלה:
			(1) נעשים שינויים מהותיים במערכות המאגר או בתהליכי עיבוד מידע;
			(2) נודע על סיכונים טכנולוגים חדשים הרלוונטים למערכות המאגר;
			(3) עלה צורך לכך כתוצאה מהביקורת התקופתית או מאירוע אבטחה אחר כאמור בתקנה 11.
			(ו) ארגון שהינו בעלים של מספר מאגרי מידע, רשאי לקיים חובה זו במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.
מיפוי וביצוע סקר סיכונים	5.		(א) בעל מאגר מידע יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מכלול רכיבי המערכות המשמשות את המאגר (להלן – מערכות המאגר), ובכלל זה -
			(1) תשתיות ומערכות חומרה, רכיבי תקשורת ואבטחת מידע, לרבות ציון של מיקומם הפיזי;
			(2) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;
			(3) תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן;
			(4) תיאור מבנה הרשת שבה פועל המאגר ותיאור של הקשרים בין מרכיבי המערכת השונים;
			(5) תאריך עדכון אחרון של המסמך ושל הרשימה.

		(ב) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר בלתי תלוי לאיתור סיכוני אבטחת מידע ומבדקי חדירות (להלן - סקר סיכונים) בהתאם לשיטה מקובלת; תוצאות סקר הסיכונים יועברו לבעל המאגר, אשר ידון בהם ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו.
		(ג) רשימת מצאי וסקר סיכונים ייערכו אחת לשמונה עשר חודשים לפחות.
		(ד) רשימת מצאי תישמר כך שפרטים ממנה יימסרו לעובדים רק בהיקף הנדרש לצורך ביצוע תפקידם.
אבטחה פיזית וסביבתית	6.	(א) בעל המאגר יבטיח כי המערכות המפורטות בתקנה 5(א)(1) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו;
		(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - ינקוט בעל המאגר אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות מערכות המאגר (בתקנות אלה – מתקני המאגר) ושל הכנסה והוצאה של ציוד אל מתקני המאגר ומהם.
אבטחת מידע בניהול כח אדם	7.	(א) לא יתן בעל מאגר לעובד גישה למידע המצוי במאגר, אלא אם נקט אמצעים סבירים לבירור כי אין חשש שהעובד אינו מתאים לקבלת גישה למידע המצוי במאגר; אמצעים אלה יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקיד שאליו מיועד העובד הנוגע בדבר, כאמור בתקנה 8.
		(ב) בעל מאגר יקיים הדרכות לעובדים בנושא החובות לפי החוק ותקנות אלה, בטרם יקבלו גישה למידע ממאגר המידע או בטרם שינוי היקף הרשאותיהם, ימסור להם מידע אודות חובותיהם לפי החוק ובהתאם לנוהל האבטחה וינקוט אמצעים סבירים לתיעוד ביצוע האמור;
		(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - יקיים בעל המאגר פעילות הדרכה תקופתית לעובדיו, בדבר הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידם, ובדבר חובות העובדים לפיהם; הדרכה כאמור תבוצע אחת לשנה לפחות, ולגבי הסמכה של עובד לתפקיד חדש – סמוך ככל האפשר למועד תחילת הסמכתו.

ניהול הרשאות גישה	8.	(א) הרשאות הגישה של עובדים למאגר המידע, תשתיות המיחשוב התקשורת ואבטחת המידע ייקבעו על בסיס הגדרת תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.
		(ב) בעל המאגר ינהל רישום מעודכן של תפקידים, הרשאות הגישה שנקבעו להם, ועובדים הממלאים תפקידים אלה (להלן – רשימת ההרשאות התקפות).
זיהוי ואימות	9.	(א) בעל המאגר יישם אמצעים לוידוא כי הגישה למידע במאגר המידע נעשית רק בידי עובד המורשה לכך ובהתאם לרשימת ההרשאות התקפות.
		(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע נוהל האבטחה הוראות לעניין האמצעים כאמור בתקנת משנה (א), ובכלל זה לנושאים אלה:

(1) אופן ביצוע הזיהוי, שייעשה ככל הניתן על בסיס אמצעי פיזי הניתן לשליטתו הבלעדית של המורשה; במידה שאופן הזיהוי מבוסס על סיסמאות יתייחס הנוהל גם לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיקבע בהתאם לתפקיד של מורשה הגישה, ובכל מקרה לא תעלה על ששה חודשים.

(2) ניתוק אוטומטי לאחר פרק זמן של אי פעילות.

(3) אופן הטיפול בתקלות הקשורות באימות זהות;

		(ג) בעל המאגר ידאג לביטול ההרשאות של עובד שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות התומכות במאגר, שהעובד עשוי היה לדעת, מיד עם סיום תפקידו של העובד.
בקרה ותיעוד גישה	10.	(א) במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה ינוהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת הגישה למערכות המאגר (בתקנה זו – מנגנון הבקרה), ובכלל זה את כל הנתונים האלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, והאם הגישה אושרה או נדחתה; אם הגישה אושרה, יישמרו הנתונים המאפשרים זיהוי רכיב המערכת שאליו בוצעה הגישה.
		(ב) מנגנון הבקרה לא יאפשר, ככל הניתן, ביטול או שינוי של הפעלתו. מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.

		(ג) בעל המאגר יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דו"ח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.
		(ד) נתוני הרישום של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.
		(ה) בעל המאגר יידע את העובדים במאגר בדבר קיומו של מנגנון הבקרה למערכות המאגר והיקף התיעוד המבוצע על ידו.
תיעוד של אירועי אבטחה	11.	(א) בעל המאגר אחראי לתיעוד אירועים המעלים חשש לפגיעה בשלמות המידע או לשימוש בו בלא הרשאה (להלן - אירועי אבטחה); ככל הניתן יבוסס התיעוד האמור על רישום אוטומטי.
		(ב) בנוהל האבטחה יקבע בעל המאגר הוראות לעניין התמודדות עם אירועי אבטחת מידע, בהתאם לחומרת האירוע ולמידת רגישות המידע, לרבות הוראות לעניין ביטול הרשאות וצעדים מיידים אחרים הנדרשים ולעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.
		(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר דיון תקופתי באירועי האבטחה.
		(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור בתקנת משנה (ג) אחת לרבעון לפחות.
		(ה) ארע אירוע אבטחה חמור, יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע. בתקנת משנה זו ובתקנת משנה (ו) – "אירוע אבטחה חמור" – א. במאגר מידע שחלה עליו רמת האבטחה הגבוהה – אירוע בו נעשה שימוש במידע מהמאגר בלא הרשאה; ב. במאגר מידע שחלה עליו רמת האבטחה הבינונית - אירוע בו נעשה שימוש בחלק מהותי של המידע מהמאגר בלא הרשאה. (ו) ארע אירוע אבטחה חמור, רשאי הרשם להורות לבעל המאגר, למעט לבעל מאגר מידע המנוי בסעיף 13(ה) לחוק, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.
התקנים ניידים	12.	(א) בעל מאגר המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד; לעניין זה, שימוש בשיטות הצפנה מקובלות ייחשב כנקיטת אמצעים סבירים.

ניהול מאובטח ומעודכן של מערכות המאגר	13.	(א) בעל המאגר יקפיד על ניהול ותפעול תקין של מערכות המידע המשמשות לביצוע פעולות במאגר, בהתאם למקובל בהפעלת מערכות אלה.
		(ב) בעל המאגר יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר.
		(ג) בעל המאגר ידאג לכך שיתבצעו עדכונים שוטפים של המערכות והתוכנות המשמשות לגישה אל המידע במאגר המידע ולהגנה עליו, לרבות חומר המחשב הנדרש לפעולתן.
אבטחת תקשורת	14.	(א) מערכות המאגר לא יחוברו לרשת האינטרנט או לרשת ציבורית אחרת ללא התקנת אמצעי הגנה מתאימים המגנים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.
		(ב) העברת מידע ממאגר המידע ברשת תקשורת אלחוטית, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.
		(ג) במאגר מידע שניתן לגשת אליו מרחוק באמצעות רשת תקשורת, בנוסף לאמצעי אבטחה כאמור בתקנות משנה (א) ו-(ב), יעשה שימוש באמצעים שמטרתם לזהות את המתקשר ומאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של עובד למאגר מידע ברמה הבינונית ייעשה שימוש באמצעי פיזי הניתן לשליטתו הבלעדית של העובד.
מיקור חוץ	15.	(א) בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, אשר כרוך במתן גישה למאגר המידע (להלן בתקנה זו - השירות) -
		(1) יבחן לפני ביצוע ההתקשרות כאמור את סיכוני אבטחת המידע הכרוכים בהתקשרות עם הגורם החיצוני המסוים;
		(2) יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה, בשים לב לסיכונים לפי תקנת משנה (1):
		(א) המידע שרשאי הגורם החיצוני לעבד ומטרות השימוש המותרות בו לצרכי ההתקשרות;
		(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;

					(ג) תכלית השימוש במידע, סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;
					(ד) משך תוקפה של ההתקשרות; אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל המאגר;
					(ה) החובות בתחום אבטחת המידע החלות על הגורם החיצוני לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל המאגר, ככל שקבע;
					(ו) חובתו של הגורם החיצוני להחתים את עובדיו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק בהתאם לאמור בהסכם וליישם את אמצעי האבטחה הקבועים בהסכם, כאמור בפסקת משנה (ה);
					(ז) אם בעל המאגר מתיר לגורם החיצוני לבצע השירות באמצעות גורם נוסף – חובתו של הגורם החיצוני לכלול בהסכם עם גורם זה את כל הנושאים המפורטים בתקנה זו;
					(ח) חובתו של הגורם החיצוני לדווח אחת לשנה לפחות לבעל המאגר אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע כאמור בתקנה 11.
				(3) יפרט בנוהל האבטחה של המאגר את העניינים המנויים בפסקה (2)(א) עד (ה), וכן יפנה בצורה מפורשת להסכם ולנוהל האבטחה של הגורם החיצוני.	
				(4) בעל המאגר ינקוט אמצעי בקרה ופיקוח כדי לוודא את עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה בהיקף הנדרש בשים לב לסיכונים בתקנה משנה (1).	
			(ב) תקנה זו לא תחול על עובד.		
ביקורות תקופתיות	16.	(א)במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, תיערך פעם בשנתיים לפחות, ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שתוודא את עמידתו בהוראות תקנות אלה.			

		(ב) אם נערכת ביקורת פנימית, לא יהיה המבקר מי שנושא בתפקיד ממונה אבטחה של המאגר.
		(ג) דו"ח הביקורת ידווח על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב, ויסתמך גם על ממצאים ממערכות המחשוב של בעל המאגר.
		(ד) דוחות הביקורת יועברו לבעל המאגר, אשר ידון בהם ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהם.
גיבוי, שחזור והתאוששות	17.	(א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע בעל המאגר -
		(1) נהלי עבודה לביצוע גיבויים מאובטחים של המידע הנצבר לצורך עמידה בהוראות תקנה 6(ב), 8 עד 12, 14, 15(א)(4) ו- 16 באופן תקופתי שגרתי;
		(2) נהלי התאוששות, כדי להבטיח שבכל עת ניתן יהיה לשחזר את המידע האמור בתקנה (1) למצבו המקורי ובלבד שביצוע השחזור יהיה באישור מנהל המאגר. בתקנה זו- "גיבוי מאובטח" – גיבוי שאין בו כדי לפגוע ברמת אבטחת המידע של המידע המגובה.
		(3) במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11, יתועדו גם הליכי שחזור המידע לפי תקנה זו, ובכלל זה יתועדו זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.
		(ב) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יישמר עותק גיבוי של המידע ושל נהלי ההתאוששות כאמור בתקנת משנה (א)(2), אשר מתקיימות גם לגביו דרישות אבטחת המידע לפי תקנות אלה, מחוץ למתקני המאגר, או שייעשה שימוש באמצעים שיבטיחו את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אובדן או הרס.
חובות על מנהל מאגר ומחזיק וחובת תיעוד	18.	(א) החובות הקבועות בתקנות אלה על בעל מאגר, יחולו גם על מנהל המאגר.

		(ב) החובות הקבועות בתקנות אלה על בעל מאגר, למעט החובות הקבועות בתקנות 2 ו-15(א), יחולו גם על המחזיק, בשינויים המחויבים ולפי העניין.
		(ב) מי שמוטלת עליו בתקנות אלה חובה או אחריות לביצוע פעולה (להלן – חובה) נדרש לתעד באופן סביר את ביצוע הפעולה, ואת הקשר בינה לבין הגדרות המאגר או נהלי המאגר לפי העניין ; הרשם רשאי לקבוע הוראות לעניין אופן תיעוד כאמור.
סמכויות הרשם	19.	(א) הרשם רשאי, בהודעה בכתב לבעל המאגר, לפטור מאגר מסוים מחובות אבטחת מידע לפי תקנות אלה, או להחיל על מאגר מסויים חובות לפי תקנות אלה, כולן או חלקן, בין היתר בהתחשב בגודל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר, או מספר העובדים במאגר ; בהודעה כאמור יקבע הרשם את המועד לתחילת הפטור או ההחלה, לפי העניין, ויכול שיקבע מועדים שונים לעניין תקנות שונות.
		(ב) הרשם רשאי להורות כי מי שיעמוד בהוראות תקן מקובל או בהנחיות של רשות מוסמכת בעניין אבטחת מידע החלות עליו, יראו אותו כמקיים הוראות תקנות אלה, כולן או חלקן, אם השתכנע כי עמידה בהוראות תקן מקובל או הנחיות רשות מוסמכת אלה, לפי העניין, באופן שקבע הרשם בהתאם לתקנות אלה, מבטיחה את רמת האבטחה הקבועה בתקנות אלה לגבי אותו מאגר מידע ; לעניין זה -
		"רשות מוסמכת" - גוף ציבורי המוסמך על פי דין לתת הנחיות בעניין אבטחת מידע ;
		"תקן מקובל" – תקן אבטחת מידע שהוא תקן ישראלי או תקן של גוף מוכר שאיננו ישראלי, שהרשם אישר לעניין זה.
תחולה	20.	(א) על מאגרי מידע שאינם מאגרים שחלה עליהם רמת האבטחה הבינונית או רמת האבטחה הגבוהה - יחולו הוראות תקנות אלה, למעט תקנות 4(ד), 5(ב), 6(ב), 7(ג), 9(ב), 10, 11(ג) עד (ד),16, 17.
		(ב) על מאגרים שחלה עליהם רמת האבטחה הבינונית - יחולו הוראות תקנות אלה, למעט תקנות 5(ב), 11(ד) ו- 17(ב).
		(ג) על מאגרים שחלה עליהם רמת האבטחה הגבוהה - יחולו בנוסף להוראות התקנות החלות על מאגרים שחלה עליהם רמת האבטחה הבינונית, גם הוראות תקנות 5(ב), 11(ד) ו- 17(ב).

פטור מתחולה	21.	על אף הוראות תקנות אלה, על מאגר מידע המנוהל על ידי יחיד שאינו תאגיד אשר הוא היחיד שמאגר המידע מצוי ברשותו, שרשאי לעשות בו שימוש ושבאפשרותו לעשות בו שימוש, לא יחולו הוראות תקנות 3, 4, 5(ב), 6(ב), 7, 8, 9(ב), 10, 16, 17.
הוראת מעבר+ביטול תקנות קיימות	22.	(א) תחילתן של תקנה 1, 3(ב), 6(א), 7(א), 8, 9(א), 9(ג), 11(ה)-(ו), 13(א), 15(א)(1), 15(א)(2), 16, 18, 19, 20, 21– 30 ימים מיום פרסום התקנות. (ב) תחילתן של תקנה 2, 3(א), 3(ג), 3(ד), 5(א), 12, 13(ב), 14, 15(א)(4) – 90 ימים מיום פרסום התקנות. (ג) תחילתן של תקנה 3(ה), 4, 5(ב), 6(ב), 7(ב), 7(ג), 9(ב), 10, 11(א)-(ד), 15(א)(3), 17 – שישה חודשים מיום פרסום התקנות.
		תוספת ראשונה
		(תקנה 1)
	1.	מאגרי מידע שחלה עליהם רמת האבטחה הבינונית:
		(1) מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר;
		(2) מאגר מידע שבעליו הוא גוף ציבורי כמשמעותו בסעיף 23 לחוק;
		(3) מאגר מידע הכולל מידע שהוא אחד מאלה:

			(א) מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד; (ב) מידע רפואי או מידע על מצבו הנפשי של אדם; (ג) מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000; (ד) מידע אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם; (ה) מידע אודות עברו הפלילי של אדם; (ו) נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח – 2007; (ז) מידע שהוא מאפיין אנושי פיזיולוגי, ייחודי, הניתן למדידה ממוחשבת, המשמש לזיהוי אדם; (ח) מידע כלכלי על אדם, לרבות מידע אודות הרגלי הצריכה של אדם;
	2.		על אף האמור בפרט 1(3) לתוספת זו, על מאגר מידע המקיים אחד מאלו, לא חלה רמת האבטחה הבינונית -
			(1) המאגר כולל מידע מן הסוגים המפורטים בפרט 1(3)(ב), (ה), (ו),(ז), (ח) לתוספת זו, אודות המועסקים או הספקים של בעל מאגר המידע, ובלבד שהמידע משמש למטרות ניהול העסק בלבד, ושהמאגר אינו כולל מידע מן הסוגים המפורטים בפרטים (א), (ג) ו-(ד);
			(2) מספר המועסקים אצל בעל המאגר אינו עולה על עשרה;
	3.		מחזיק במאגרי מידע מן הסוגים המפורטים בפסקה 1, השייכים לחמישה בעלים שונים לפחות.
			תוספת שניה
			(תקנה 1)
			מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה:
			(1) מאגר מידע כאמור בפרט 1 לתוספת הראשונה, שיש בו מידע אודות 100,000 אנשים ומעלה.

		(2) מאגר מידע כאמור בפרט 1 לתוספת הראשונה שמספר מורשי הגישה למידע במאגר עולה על 100.